PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-208921
(43)Date of publication of application : 26.07.2002

(51)Int.Cl. H04L 9/08
G06F 15/00
H04L 9/32

(21)Application number : 2001-151279
(22)Date of filing : 21.05.2001

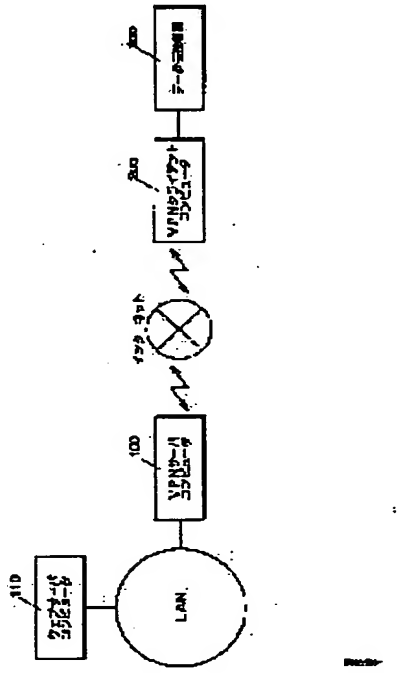
(71)Applicant : NIPPON TELEGRAPH & TELEPHONE EAST CORP
HITACHI SYSTEMS & SERVICES LTD

(72)Inventor : ENDO HISASHI
SHIBAYAMA HIROKO
OKADA KENICHI
KOSAKA TATSUYA
GENDA KOICHI
UENO KEIJI

(30)Priority
Priority number : 2000340853 Priority date : 08.11.2000 Priority country : JP

(54) VPN DATA COMMUNICATION METHOD AND PRIVATE NETWORK CONSTRUCTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a VPN construction system which can construct a VPN without restriction by an IP address and access to a VPN server.
SOLUTION: In a portable data transmission device 300, a coding key used for coding treatment by a VPN client 200, a decoding key specific information for specifying a decoding key for decoding data coded by the VPN client 200, if received by a VPN server 100, and VPN transmission base data including an IP address of a VPN server are stored. The VPN client 200 reads transmission foundation data and stores it in a memory when the data transmission device 300 is connected. Thereby, transmission base data is not transferred on internet and data transmission is possible while keeping privacy.



LEGAL STATUS

[Date of request for examination] 22.05.2001
[Date of sending the examiner's decision of rejection] 07.03.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	2005-05938
[Date of requesting appeal against examiner's decision of rejection]	06.04.2005
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－208921
（P2002－208921A）
(43)公開日　平成14年７月26日(2002.7.26)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｈ０４Ｌ　9/00	６０１Ｃ	５Ｊ１０４
Ｈ０４Ｌ　9/32			６７３Ｄ	

審査請求　有　　請求項の数13　ＯＬ　（全 22 頁）

(21)出願番号　特願2001－151279(P2001－151279)

(22)出願日　平成13年５月21日(2001.5.21)

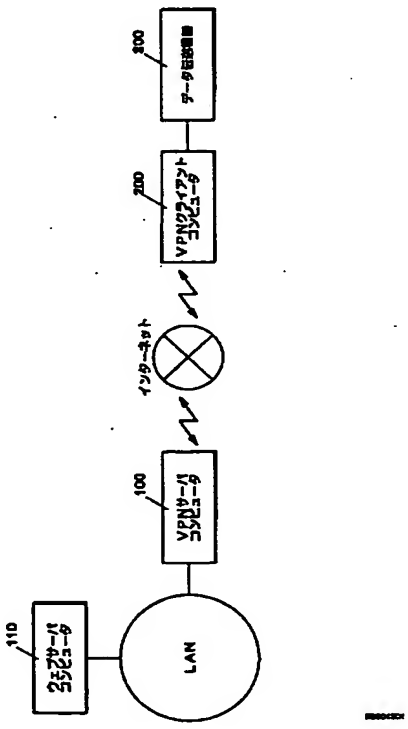
(31)優先権主張番号　特願2000－340853(P2000－340853)
(32)優先日　平成12年11月８日(2000.11.8)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　399040405
東日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(71)出願人　391002409
株式会社　日立システムアンドサービス
東京都大田区大森北３丁目２番16号
(72)発明者　遠藤　久
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(74)代理人　100092956
弁理士　古谷　栄男　（外２名）

最終頁に続く

(54)【発明の名称】　ＶＰＮデータ通信方法および私設網構築システム

(57)【要約】
【課題】　ＩＰアドレスに拘束されず、かつ、ＶＰＮサーバにアクセスすることなく、ＶＰＮを構築できるＶＰＮ構築システムを提供する。
【解決手段】　携行可能なデータ伝送機器３００は、ＶＰＮクライアント２００にて暗号化処理に用いる暗号化キー、ＶＰＮクライアント２００によって暗号化されたデータをＶＰＮサーバ１００が受信した場合に、これを復号化する復号化キーを特定する復号化キー特定情報、およびＶＰＮサーバのＩＰアドレスを含むＶＰＮ伝送基礎データを記憶している。ＶＰＮクライアント２００は、データ伝送機器３００が接続されると、伝送基礎データを読み出してメモリに記憶する。インターネット上を伝送基礎データが転送されず、守秘性を保持しつつ、データ伝送が可能となる。



【特許請求の範囲】
【請求項１】Ａ）ＶＰＮサーバコンピュータとＶＰＮクライアントコンピュータとの間で、ネットワークを介してＶＰＮを構築してデータ通信する方法であって、
Ｂ）ＶＰＮクライアントコンピュータとの間でデータ伝送が可能で、かつ携帯可能なデータ伝送機器に、ＶＰＮクライアントコンピュータがＶＰＮサーバコンピュータとの間でＶＰＮ伝送時に用いるＶＰＮ伝送基礎データであって、少なくとも1)ＶＰＮクライアントコンピュータにて暗号化処理に用いるＶＰＮ暗号化キーまたはＶＰＮ暗号化キーを特定するＶＰＮ暗号化キー特定情報、2)ＶＰＮサーバコンピュータで復号化処理に用いるＶＰＮ復号化キーを特定するＶＰＮ復号化キー特定情報、および3)ＶＰＮサーバコンピュータのＩＰアドレスを含むＶＰＮ伝送基礎データを記憶させておき、
Ｃ）前記データ伝送機器をＶＰＮ構築希望するＶＰＮクライアントコンピュータに接続し、
Ｄ）前記データ伝送機器から前記ＶＰＮ伝送基礎データを読み出して、前記ＶＰＮサーバコンピュータとの間で、ＶＰＮを構築し、前記ＶＰＮサーバコンピュータへデータ送信要求があると、送信対象データを前記ＶＰＮ暗号化キーを用いて暗号化して、前記ＶＰＮ復号化キー特定情報とともに前記ＶＰＮサーバコンピュータのＩＰアドレスにデータ転送し、
Ｅ）前記ＶＰＮサーバコンピュータは、前記ＶＰＮ復号化キー特定情報に基づいて、前記暗号化されたデータを復号化するキーを特定し、復号化処理すること、
を特徴とするＶＰＮデータ通信方法。
【請求項２】仮想私設網サーバコンピュータ、
ネットワークを介して前記仮想私設網サーバコンピュータと接続された仮想私設網クライアントコンピュータ、
を備え、前記仮想私設網サーバコンピュータと前記仮想私設網クライアントコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網構築システムであって、
携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも1)仮想私設網クライアントコンピュータにて暗号化処理に用いる仮想私設網暗号化キーまたは仮想私設網暗号化キー特定情報、2)仮想私設網サーバで復号化処理に用いる仮想私設網復号化キーを特定する仮想私設網復号化キー特定情報、および3)仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、
前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築すること、
を特徴とする仮想私設網構築システム。
【請求項３】仮想私設網サーバコンピュータ、
ネットワークを介して前記仮想私設網サーバコンピュータと接続された仮想私設網クライアントコンピュータ、
を備え、前記仮想私設網サーバコンピュータと前記仮想私設網クライアントコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網構築システムであって、
携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも1)仮想私設網クライアントコンピュータと仮想私設網サーバコンピュータとの暗号化データ伝送に用いる仮想私設網暗号化キーおよび仮想私設網復号化キーを特定する仮想私設網暗号化復号化キー特定情報、および2)仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、
前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して、前記仮想私設網サーバコンピュータとの暗号化データ伝送に用いる仮想私設網暗号化キーおよび仮想私設網復号化キーを特定することにより、仮想私設網を構築すること、
を特徴とする仮想私設網構築システム。
【請求項４】請求項２または請求項３の仮想私設網システムにおいて、
前記仮想私設網クライアントコンピュータは、前記仮想私設網暗号化キーを用いて暗号化して、前記仮想私設網復号化キー特定情報とともに前記仮想私設網サーバコンピュータへデータ転送し、
前記仮想私設網サーバコンピュータは前記仮想私設網復号化キー特定情報に基づいて、前記暗号化されたデータを復号化するキーを特定し、復号化処理すること、
を特徴とするもの。
【請求項５】仮想私設網サーバコンピュータとネットワークを介して接続された仮想私設網クライアントコンピュータであって、前記仮想私設網サーバコンピュータとの間で、受信した暗号化データを復号化できる復号化キーを記憶しておき、データ伝送する仮想私設網クライアントコンピュータにおいて、
携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも仮想私設網暗号化キー、仮想私設網復号化キー特定情報、および仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、

前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築すること、
を特徴とする仮想私設網クライアントコンピュータ。
【請求項６】コンピュータを、仮想私設網サーバコンピュータから受信した暗号化データを復号化できる復号化キーを記憶しておきネットワークを介して接続された仮想私設網サーバコンピュータとの間でデータ伝送する仮想私設網クライアントコンピュータとして機能させるためのコンピュータ可読のプログラムであって、以下の処理を実行する、
前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも仮想私設網暗号化キー、仮想私設網復号化キー特定情報、および仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶した携帯可能なデータ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する、ためのプログラムであることを特徴とするコンピュータ可読のプログラム。
【請求項７】クライアントコンピュータと特定のサーバコンピューター又は特定のＬＡＮとの間の通信で、クライアントコンピュータ内部またはクライアントコンピュータとネットワークとの間にＶＰＮクライアント機能を配備し、上記特定サーバ内部または特定サーバや特定ＬＡＮとネットワークとの間にＶＰＮサーバ機能を配備し、上記ＶＰＮクライアントとＶＰＮサーバ機能との間で転送されるデータを暗号化して転送するＶＰＮ通信システムにおいて、
Ａ）上記ネットワークはインターネット等の公衆ネットワークやＬＡＮであり、
Ｂ）ＶＰＮクライアント機能は携帯可能なデータ伝送機器とデータ伝送機器を動作させるドライバプログラムから構成され、
Ｃ）ＶＰＮクライアント機能のドライバプログラムは、前記データ伝送機器をＶＰＮ通信するクライアントコンピュータに接続した時、前記データ伝送機器から前記ＶＰＮ伝送基礎データをクライアントコンピュータに読み出し動作可能な状態とし、
Ｄ）前記携帯可能なデータ伝送機器には、ＶＰＮ伝送基礎データとして、d1)ＶＰＮクライアント識別情報、d2)暗号化復号化処理に必要な暗号鍵情報、d3)ＶＰＮサーバ機能を示すＩＰアドレス、d4)上記特定サーバを示すＩＰアドレスまたは特定ＬＡＮを示すＩＰサブネットアドレスを内蔵し、
Ｅ）ＶＰＮサーバ機能には、ＶＰＮサーバ識別情報、暗号化通信するすべてのＶＰＮクライアント識別情報、暗号化復号化処理に必要な暗号鍵情報を内蔵し、
Ｆ）前記ＶＰＮクライアント機能は、クライアントコンピュータが特定のサーバコンピューターまたは特定のＬＡＮへ向けてデータ送信する時、ＶＰＮサーバ機能との間でお互いのＶＰＮ伝送基礎データをやりとりすることによりＶＰＮを確立し、送信対象データを前記ＶＰＮ伝送基礎データを用いて暗号化し、前記ＶＰＮサーバ機能を示すＩＰアドレスにデータを転送し、
Ｇ）前記ＶＰＮサーバ機能は、前記ＶＰＮクライアント機能と通信するためのＶＰＮ伝送基礎データに基づいて、前記暗号化されたデータを復号化する暗号鍵を用いて復号した後、前記特定のサーバコンピューターまたは特定のＬＡＮへデータを転送すること、
を特徴とするＶＰＮ通信システム。
【請求項８】請求項２または請求項３の仮想私設網システムにおいて、
前記データ伝送機器には、仮想私設網クライアントコンピュータ用のプログラムが記録されており、前記仮想私設網クライアントコンピュータは、当該プログラムを読み出して、前記仮想私設網の構築を実行すること、
を特徴とするもの。
【請求項９】コンピュータを、ネットワークを介して接続された仮想私設網サーバコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網クライアントコンピュータとして機能させるためのプログラムを記録した記録媒体であって、
前記コンピュータは、前記プログラムを記録した記録媒体が接続されると、
前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも1)仮想私設網クライアントコンピュータにて暗号化処理に用いる仮想私設網暗号化キーまたは仮想私設網暗号化キー特定情報、2)仮想私設網サーバで復号化処理に用いる仮想私設網復号化キーを特定する仮想私設網復号化キー特定情報、および3)仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを、前記記録媒体から読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する、
ことを特徴とするコンピュータ可読のプログラムを記録した記録媒体。
【請求項１０】請求項９のプログラムを記録した記録媒体において、
前記記録媒体には、仮想私設網クライアントコンピュータ用のプログラムが記録されており、前記仮想私設網クライアントコンピュータは、当該プログラムを読み出して、前記仮想私設網の構築を実行すること、
を特徴とするもの。

【請求項１１】請求項１０のプログラムを記録した記録媒体において、
前記記録媒体は、仮想私設網クライアントコンピュータ用のプログラムおよび仮想私設網伝送基礎データが記録された仮想私設網関連データ記憶部と、前記仮想私設網関連データを読み出すための読み出しプログラムが記録された読み出しプログラム記録部とを有しており、
前記仮想私設網関連データ記憶部は、前記クライアントコンピュータのファイルシステムとは異なるデータ構造で記録されており、
前記読み出しプログラムは、使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、仮想私設網クライアントコンピュータ用のプログラムおよび仮想私設網伝送基礎データを読み出して、前記仮想私設網の構築を実行すること、
を特徴とするもの。
【請求項１２】データを記録した記録媒体を、コンピュータに接続することにより、前記コンピュータのオペレーティングシステムプログラムが、前記記録媒体に記録された仮想私設網構築プログラムを起動させ、かかる仮想私設網構築プログラムによって、前記記録媒体に記録された仮想私設網構築用データを読み出して、仮想私設網サーバコンピュータとの間で仮想私設網を構築する方法であって、
前記仮想私設網構築データは、前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記憶されており、
前記仮想私設網構築プログラムは、使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、前記仮想私設網構築データを前記隠しデータ領域から読み出して、前記仮想私設網を構築するプログラムであること、
ことを特徴とする仮想私設網を構築する方法。
【請求項１３】コンピュータを、ネットワークを介して接続された仮想私設網サーバコンピュータとの間で仮想私設網を構築した仮想私設網クライアントコンピュータとして機能させるためのプログラムを記録した記録媒体であって前記記録媒体には、
1)前記仮想私設網構築データが前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記録されており、
2)使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、前記仮想私設網構築データを前記隠しデータ領域から読み出して、前記仮想私設網を構築するプログラムが前記オペレーティングシステムプログラムが記録されているデータのデータ形式を離隔できる領域に記録されている、
ことを特徴とするプログラムを記録したコンピュータ可読の記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、ＶＰＮに関し、特に、コンピュータのＩＰアドレスに依存しないＶＰＮクライアントコンピュータに関する。
【０００２】
【従来技術】今日、バーチャルプライベートネットワーク（以下ＶＰＮと略す）が注目されている。これは、ネットワークを介しても、守秘性の高いネットワークを個人単位で構築する技術である。図１４を用いて、簡単に説明する。
【０００３】Ａ社の会計処理サーバコンピュータ５００には社内ＬＡＮを介してＶＰＮサーバコンピュータ５０３が接続されている。Ｂ社の端末コンピュータ６０３には、ＶＰＮクライアントプログラムがインストールされている。ＶＰＮサーバコンピュータ５０３および端末コンピュータ６０３双方には、ＶＰＮを形成するためのＶＰＮデータが記憶されている。端末の操作者は、ＶＰＮクライアントプログラムを実行して、ＶＰＮサーバコンピュータ５０３との間で、ＶＰＮを構築する命令を端末コンピュータ６０３に与える。端末コンピュータ６０３は、かかる命令を受けて、記憶されているＶＰＮデータを用いて、ＶＰＮサーバコンピュータ５０３との間で、仮想的に、ネットワークを構築する。具体的には、端末５０３と会計処理サーバコンピュータ５００との間のデータのやりとりは、前記ＶＰＮデータに含まれる暗号化処理データを用いて、暗号化されて実行される。このように、予め登録されたコンピュータ間のデータ伝送をＶＰＮサーバコンピュータを介して行うことにより、ネットワークを介しても、個人レベルで守秘性の高い伝送が可能となる。
【０００４】
【発明が解決しようとする課題】しかしながら、ＶＰＮの構築には以下のような問題があった。例えば、前記端末コンピュータ６０３の操作者が、出張のために、別のコンピュータと会計処理サーバコンピュータ５００との間で守秘性の高いデータ伝送をさせる場合には、予め当該コンピュータおよび会計処理サーバコンピュータ５００にＶＰＮデータを記憶させておかなければならない。
【０００５】かかる問題を解決するために、特開２０００－５９３５７号公報に開示されているように、各ユーザについてＩＤおよびパスワードを記録したＩＣカードを発行し、前記ＩＤおよびパスワードを用いて管理サーバコンピュータにアクセスし、ＶＰＮサーバコンピュータで用いる公開鍵および自己の秘密鍵を取得して、ＶＰＮ情報を取得してＶＰＮを構築することも考えられる。しかし、これでは、ＶＰＮを構築する場合には、自己の秘密鍵がネットワーク上を転送されるので、自己の秘密鍵が第三者に取得されるおそれがある。特に、ネットワ

ークとしてインターネットというオープンなネットワークを介在させる場合に、より第三者への情報の漏れが問題となる。

【０００６】また、ＶＰＮを構築する都度、管理サーバコンピュータにアクセスする必要があり、管理サーバコンピュータが混雑している場合には、ＶＰＮ構築に時間がかかる。

【０００７】この発明は、仮想私設網の構築情報について守秘性を保持しつつ、仮想私設網の対象となるコンピュータの柔軟性を向上させたネットワークを用いた仮想私設網を構築することができる仮想私設網構築システムを提供することを目的とする。さらに、簡易に仮想私設網を構築できる仮想私設網構築システムを提供することを目的とする。

【０００８】

【課題を解決するための手段および発明の効果】１）本発明にかかるＶＰＮデータ通信方法においては、Ａ）ＶＰＮサーバコンピュータとＶＰＮクライアントコンピュータとの間で、ネットワークを介してＶＰＮを構築してデータ通信する方法であって、Ｂ）ＶＰＮクライアントコンピュータとの間でデータ伝送が可能で、かつ携帯可能なデータ伝送機器に、ＶＰＮクライアントコンピュータがＶＰＮサーバコンピュータとの間でＶＰＮ伝送時に用いるＶＰＮ伝送基礎データであって、少なくとも1)ＶＰＮクライアントコンピュータにて暗号化処理に用いるＶＰＮ暗号化キーまたはＶＰＮ暗号化キーを特定するＶＰＮ暗号化キー特定情報、2)ＶＰＮサーバコンピュータで復号化処理に用いるＶＰＮ復号化キーを特定するＶＰＮ復号化キー特定情報、および3)ＶＰＮサーバコンピュータのＩＰアドレスを含むＶＰＮ伝送基礎データを記憶させておき、Ｃ）前記データ伝送機器をＶＰＮ構築希望するＶＰＮクライアントコンピュータに接続し、Ｄ）前記データ伝送機器から前記ＶＰＮ伝送基礎データを読み出して、前記ＶＰＮサーバコンピュータとの間で、ＶＰＮを構築し、前記ＶＰＮサーバコンピュータへデータ送信要求があると、送信対象データを前記ＶＰＮ暗号化キーを用いて暗号化して、前記ＶＰＮ復号化キー特定情報とともに前記ＶＰＮサーバコンピュータのＩＰアドレスにデータ転送し、Ｅ）前記ＶＰＮサーバコンピュータは、前記ＶＰＮ復号化キー特定情報に基づいて、前記暗号化されたデータを復号化するキーを特定し、復号化処理する。

【０００９】このように、携帯可能なデータ伝送機器にＶＰＮ伝送基礎データを記憶させておき、ＶＰＮ構築希望のＶＰＮクライアントコンピュータに接続させて、ＶＰＮを構築することにより、予めＶＰＮ伝送基礎データを記憶させていないＶＰＮクライアントコンピュータであっても、ＶＰＮ構築が可能となる。また、前記データ伝送機器に暗号化キーを記憶させているので、ＶＰＮクライアントコンピュータで用いる暗号化キーがネットワーク上を転送されることによるセキュリティー低下の問題もない。また、ＶＰＮ復号化キー特定情報およびＶＰＮサーバコンピュータのＩＰアドレスを記憶しているので、ＶＰＮサーバコンピュータにアクセスすることなく、ＶＰＮを構築することができる。

【００１０】２）本発明にかかる仮想私設網システムにおいては、Ａ）仮想私設網サーバコンピュータ、Ｂ）ネットワークを介して前記仮想私設網サーバコンピュータと接続された仮想私設網クライアントコンピュータを備え、Ｃ）前記仮想私設網サーバコンピュータと前記仮想私設網クライアントコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網構築システムであって、Ｄ）携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくともd1)仮想私設網クライアントコンピュータにて暗号化処理に用いる仮想私設網暗号化キーまたは仮想私設網暗号化キーを特定する仮想私設網暗号化キー特定情報、d2)仮想私設網サーバで復号化処理に用いる仮想私設網復号化キーを特定する仮想私設網復号化キー特定情報、およびd3)仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、Ｅ）前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する。

【００１１】このように、携帯可能なデータ伝送機器に仮想私設網伝送基礎データを記憶させておき、仮想私設網構築希望の仮想私設網クライアントコンピュータに接続させて、仮想私設網を構築することにより、予め仮想私設網伝送基礎データを記憶させていない仮想私設網クライアントコンピュータであっても、仮想私設網構築が可能となる。また、前記データ伝送機器に暗号化キーを記憶させているので、ネットワーク上を暗号化キーが転送されることによるセキュリティー低下の問題もない。また、仮想私設網復号化キー特定情報および仮想私設網サーバコンピュータのコンピュータ特定データを記憶しているので、仮想私設網サーバにアクセスすることなく、仮想私設網を構築することができる。

【００１２】３）本発明にかかる仮想私設網システムにおいては、Ａ）仮想私設網サーバコンピュータ、Ｂ）ネットワークを介して前記仮想私設網サーバコンピュータと接続された仮想私設網クライアントコンピュータを備え、Ｃ）前記仮想私設網サーバコンピュータと前記仮想私設網クライアントコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網構築システムであって、Ｄ）携帯可能なデータ伝送機器に、前記仮想私

設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくともd1)仮想私設網クライアントコンピュータと仮想私設網サーバコンピュータとの暗号化データ伝送に用いる仮想私設網暗号化キーおよび仮想私設網復号化キーを特定する仮想私設網暗号化復号化キー特定情報、およびd2)仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、Ｅ）前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して、前記仮想私設網サーバコンピュータとの暗号化データ伝送に用いる仮想私設網暗号化キーおよび仮想私設網復号化キーを特定することにより、仮想私設網を構築する。

【００１３】このように、携帯可能なデータ伝送機器に仮想私設網伝送基礎データを記憶させておき、仮想私設網構築希望の仮想私設網クライアントコンピュータに接続させて、仮想私設網を構築することにより、予め仮想私設網伝送基礎データを記憶させていない仮想私設網クライアントコンピュータであっても、仮想私設網構築が可能となる。また、前記データ伝送機器に暗号化キーを特定する特定情報を記憶させているので、ネットワーク上を暗号化キーが転送されることによるセキュリティー低下の問題もない。

【００１４】４）本発明にかかる仮想私設網システムにおいては、前記仮想私設網クライアントコンピュータは、前記仮想私設網サーバコンピュータへのデータ送信要求があると、送信対象データを前記仮想私設網暗号化キーを用いて暗号化して、前記仮想私設網復号化キー特定情報とともに前記仮想私設網サーバへデータ転送し、前記仮想私設網サーバコンピュータは、前記仮想私設網復号化キー特定情報に基づいて、前記暗号化されたデータを復号化するキーを特定し、復号化処理する。これにより、ＶＰＮを用いたデータ通信が可能となる。

【００１５】５）本発明にかかる仮想私設網クライアントコンピュータにおいては、Ａ）仮想私設網サーバコンピュータとネットワークを介して接続された仮想私設網クライアントコンピュータであって、前記仮想私設網サーバコンピュータとの間で、受信した暗号化データを復号化できる復号化キーを記憶しておき、データ伝送する仮想私設網クライアントコンピュータであって、Ｂ）携帯可能なデータ伝送機器に、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくともb1)仮想私設網暗号化キーまたは仮想私設網暗号化キーを特定する仮想私設網暗号化キー特定情報、b2)仮想私設網復号化キー特定情報、およびb3)仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを記憶させておき、Ｃ）前記仮想私設網クライアントコンピュータは、前記データ伝送機器が接続されると、前記仮想私設網伝送基礎データを読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する。

【００１６】このように、携帯可能なデータ伝送機器に仮想私設網伝送基礎データを記憶させておき、仮想私設網構築希望の仮想私設網クライアントコンピュータに接続させて、仮想私設網を構築することにより、予め仮想私設網伝送基礎データを記憶させていない仮想私設網クライアントコンピュータであっても、仮想私設網構築が可能となる。また、前記データ伝送機器に暗号化キーを記憶させているので、ネットワーク上を暗号化キーが転送されることによるセキュリティー低下の問題もない。また、仮想私設網復号化キー特定情報および仮想私設網サーバコンピュータのコンピュータ特定データを記憶しているので、仮想私設網サーバにアクセスすることなく、仮想私設網を構築することができる。

【００１７】７）本発明にかかるＶＰＮ通信システムにおいては、クライアントコンピュータと特定のサーバコンピューター又は特定のＬＡＮとの間の通信で、クライアントコンピュータ内部またはクライアントコンピュータとネットワークとの間にＶＰＮクライアント機能を配備し、上記特定サーバ内部または特定サーバや特定ＬＡＮとネットワークとの間にＶＰＮサーバ機能を配備し、上記ＶＰＮクライアントとＶＰＮサーバ機能との間で転送されるデータを暗号化して転送するＶＰＮ通信システムにおいて、Ａ）上記ネットワークはインターネット等の公衆ネットワークやＬＡＮであり、Ｂ）ＶＰＮクライアント機能は携帯可能なデータ伝送機器とデータ伝送機器を動作させるドライバプログラムから構成され、Ｃ）ＶＰＮクライアント機能のドライバプログラムは、前記データ伝送機器をＶＰＮ通信するクライアントコンピュータに接続した時、前記データ伝送機器から前記ＶＰＮ伝送基礎データをクライアントコンピュータに読み出し動作可能な状態とし、Ｄ）前記携帯可能なデータ伝送機器には、ＶＰＮ伝送基礎データとして、d1)ＶＰＮクライアント識別情報、d2)暗号化復号化処理に必要な暗号鍵情報、d3)ＶＰＮサーバ機能を示すＩＰアドレス、d4)上記特定サーバを示すＩＰアドレスまたは特定ＬＡＮを示すＩＰサブネットアドレスを内蔵し、Ｅ）ＶＰＮサーバ機能には、ＶＰＮサーバ識別情報、暗号化通信するすべてのＶＰＮクライアント識別情報、暗号化復号化処理に必要な暗号鍵情報を内蔵し、Ｆ）前記ＶＰＮクライアント機能は、クライアントコンピュータが特定のサーバコンピューターまたは特定のＬＡＮへ向けてデータ送信する時、ＶＰＮサーバ機能との間でお互いのＶＰＮ伝送基礎データをやりとりすることによりＶＰＮを確立し、送信対象データを前記ＶＰＮ伝送基礎データを用いて暗号化し、前記ＶＰＮサーバ機能を示すＩＰアドレスにデータを転送し、Ｇ）前記ＶＰＮサーバ機能は、

前記ＶＰＮクライアント機能と通信するためのＶＰＮ伝送基礎データに基づいて、前記暗号化されたデータを復号化する暗号鍵を用いて復号した後、前記特定のサーバコンピューターまたは特定のＬＡＮへデータを転送する。

【００１８】このように、携帯可能なデータ伝送機器にＶＰＮ伝送基礎データを記憶させておき、ＶＰＮ構築希望のクライアントコンピュータに接続させてＶＰＮを構築することにより、クライアントコンピュータがＶＰＮ通信に必要な暗号鍵がネットワーク上を転送されることによるセキュリティ低下の問題がない。またＶＰＮ伝送基礎データを携帯しているため、ＶＰＮ通信のたびにＶＰＮクライアント機能からＶＰＮサーバ機能にアクセスする必要がなく、ＶＰＮサーバ機能の処理負荷を低減できる。

【００１９】８）本発明にかかる仮想私設網システムにおいては、前記データ伝送機器には、仮想私設網クライアントコンピュータ用のプログラムが記録されており、前記仮想私設網クライアントコンピュータは、当該プログラムを読み出して、前記仮想私設網の構築を実行する。したがって、前記仮想私設網クライアントコンピュータ用のプログラムが記録されていないコンピュータであっても、前記データ伝送機器を接続するだけで、仮想私設網クライアントコンピュータとして機能させることができる。

【００２０】９）本発明にかかる記録媒体においては、コンピュータを、ネットワークを介して接続された仮想私設網サーバコンピュータとの間で、暗号化されたデータを受信して復号化する復号化キーをお互いに記憶しておき、データ伝送する仮想私設網クライアントコンピュータとして機能させるためのプログラムを記録した記録媒体であって、前記コンピュータは、前記プログラムを記録した記録媒体が接続されると、前記仮想私設網クライアントコンピュータが前記仮想私設網サーバコンピュータとの間で仮想私設網を構築する場合に用いる仮想私設網伝送基礎データであって、少なくとも1)仮想私設網クライアントコンピュータにて暗号化処理に用いる仮想私設網暗号化キーまたは仮想私設網暗号化キー特定情報、2)仮想私設網サーバで復号化処理に用いる仮想私設網復号化キーを特定する仮想私設網復号化キー特定情報、および3)仮想私設網サーバコンピュータのコンピュータ特定データを含む仮想私設網伝送基礎データを、前記記録媒体から読み出して前記仮想私設網サーバコンピュータとの間で、仮想私設網を構築する。したがって、前記仮想私設網伝送基礎データを有していないコンピュータであっても、前記データ伝送機器を接続すれば、仮想私設網を構築することができる。

【００２１】１０）本発明にかかる記録媒体においては、仮想私設網クライアントコンピュータ用のプログラムが記録されており、前記仮想私設網クライアントコンピュータは、当該プログラムを読み出して、前記仮想私設網の構築を実行する。したがって、前記仮想私設網クライアントコンピュータ用のプログラムが記録されていないコンピュータであっても、前記データ伝送機器を接続するだけで、仮想私設網クライアントコンピュータとして機能させることができる。

【００２２】１１）本発明にかかる記録媒体においては、前記記録媒体は、仮想私設網クライアントコンピュータ用のプログラムおよび仮想私設網伝送基礎データが記録された仮想私設網関連データ記憶部と、前記仮想私設網関連データを読み出すための読み出しプログラムが記録された読み出しプログラム記録部とを有しており、前記仮想私設網関連データ記憶部は、前記クライアントコンピュータのファイルシステムとは異なるデータ構造で記録されている。前記読み出しプログラムは、使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、仮想私設網クライアントコンピュータ用のプログラムおよび仮想私設網伝送基礎データを読み出して、前記仮想私設網の構築を実行する。このように、仮想私設網伝送基礎データを前記コンピュータのファイルシステムとは異なるデータ構造で記録しておき、前記読み出しプログラムを介して、仮想私設網伝送基礎データおよび仮想私設網クライアントコンピュータ用のプログラムを読み出すことにより、仮想私設網伝送基礎データおよびそのプログラムの盗み見ることから防止することができる。特に、仮想私設網クライアントコンピュータ用のプログラムを前記記録媒体に記録する場合には、かかる直接読み取りできなくすることにより、より守秘性を高めることができる。

【００２３】１１）本発明にかかる仮想私設網を構築する方法においては、データを記録した記録媒体を、コンピュータに接続することにより、前記コンピュータのオペレーティングシステムプログラムが、前記記録媒体に記録された仮想私設網構築プログラムを起動させ、かかる仮想私設網構築プログラムによって、前記記録媒体に記録された仮想私設網構築用データを読み出して、仮想私設網サーバコンピュータとの間で仮想私設網を構築する方法であって、前記仮想私設網構築データは、前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記憶されており、前記仮想私設網構築プログラムは、使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、前記仮想私設網構築データを前記隠しデータ領域から読み出して、前記仮想私設網を構築するプログラムである。このように、前記仮想私設網構築データを、前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記憶しておき、前記仮想私設網構築プログラムが前記仮想私設網構築データを読み出

すことにより、前記仮想私設網構築データを盗み見ることから防止することができる。特に、仮想私設網クライアントコンピュータ用のプログラムを前記記録媒体に記録する場合には、かかる直接読み取りできなくすることにより、より守秘性を高めることができる。

【００２４】１２）本発明にかかるプログラムを記録したコンピュータ可読の記録媒体においては、コンピュータを、ネットワークを介して接続された仮想私設網サーバコンピュータとの間で仮想私設網を構築した仮想私設網クライアントコンピュータとして機能させるためのプログラムを記録した記録媒体であって、前記記録媒体には、1)前記仮想私設網構築データが前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記録されており、2)使用者識別情報が与えられると、あらかじめ記憶されている照合情報との照合状態を検査し、照合する場合には、前記仮想私設網構築データを前記隠しデータ領域から読み出して、前記仮想私設網を構築するプログラムが前記オペレーティングシステムプログラムが記録されているデータのデータ形式を離隔できる領域に記録されている。このように、前記仮想私設網構築データを、前記オペレーティングシステムプログラムだけではデータを読み出すことができない隠しデータ領域に記憶しておき、前記仮想私設網構築プログラムが前記仮想私設網構築データを読み出すことにより、前記仮想私設網構築データを盗み見ることから防止することができる。特に、仮想私設網構築プログラムを前記記録媒体に記録して、当該記録媒体さえあれば、仮想私設網を構築できるようにする場合には、かかる直接読み取りできなくすることにより、より守秘性を高めることができる。

【００２５】なお、ＶＰＮサーバ機能からＶＰＮクライアント機能への通信も逆の手順で同様にすればよい。

【００２６】本実施形態においては、仮想私設網復号化キー特定情報として、ＶＰＮサーバ識別子およびＶＰＮクライアント識別子を用いた。これにより、１つのＶＰＮサーバについて、複数のＶＰＮサーバ識別子を設定することができる。しかし、仮想私設網復号化キー特定情報としては、ＶＰＮサーバに記憶された復号化キーのうち、いずれを用いて復号すればよいかを特定できるものであればどのようなものであってもよく、復号化キー番号などであってもよい。この場合には、ＶＰＮサーバ識別子は不要となる。

【００２７】また、ＶＰＮ暗号化方式は１つの方式に決めておけば、ＶＰＮ伝送基礎データに記憶させる必要はない。

【００２８】なお、「読み出しプログラム」とは、実施形態では、起動プログラム４１１ａが該当する。「使用者識別情報」とは、実施形態ではＩＤとパスワードが該当する。また、「仮想私設網関連データ記憶部」「読み出しプログラム記録部」は、それぞれ、領域４１２、領域４１１に該当する。また、「隠しデータ領域」とは実施形態では領域４１２に該当する。

【００２９】

【発明の実施の形態】１．概略および機能ブロックの説明

本発明の一実施形態を図面に基づいて説明する。図１に示す仮想私設網データ伝送システムは、ＶＰＮサーバコンピュータ（以下ＶＰＮサーバと略す）１００、ＶＰＮクライアントコンピュータ（以下ＶＰＮクライアントと略す）２００およびデータ伝送機器３００を備えている。

【００３０】ＶＰＮサーバ１００は、ＬＡＮでウェブサーバコンピュータ１１０に接続されている。ＶＰＮクライアント２００はインターネットなどのネットワークを介してＶＰＮサーバ１００に接続されている。ＶＰＮクライアント２００には、データ伝送機器３００が接続されている。

【００３１】本システムの主要部分の詳細機能ブロックについて、図２を用いて説明する。

【００３２】データ伝送機器３００は、送受信手段１１、判定手段１２，ＶＰＮ伝送基礎データ記憶手段１０を備えている。

【００３３】ＶＰＮ伝送基礎データ記憶手段１０は、ＶＰＮ伝送基礎データを記憶する。ＶＰＮ伝送基礎データは、少なくとも、1)ＶＰＮクライアント２００にて暗号化処理に用いるＶＰＮ暗号化キー、2)ＶＰＮクライアント２００によって暗号化されたデータをＶＰＮサーバ１００が受信した場合に、これを復号化する時に用いるＶＰＮ復号化キーを特定するＶＰＮ復号化キー特定情報、および3)ＶＰＮサーバのＩＰアドレスを含む。

【００３４】ＶＰＮクライアント２００は、接続状態制御手段６、読み出しデータ記憶手段４、報知手段７および入力手段８を備えており、データ伝送機器３００が接続されると、以下のようにして、前記ＶＰＮ伝送基礎データ記憶手段１０に記憶されたＶＰＮ伝送基礎データを読み出して、読み出しデータ記憶手段４に記憶する。

【００３５】接続状態制御手段６は、データ伝送機器３００が接続されるとこれを検出し、報知手段７によって、操作者に、操作者ＩＤおよびパスワード入力可能状態であることを報知する。操作者は、操作者ＩＤおよびパスワードを入力手段８から入力する。接続状態制御手段６は入力された操作者ＩＤおよびパスワードをデータ伝送機器３００の送受信手段１１に送信する。送受信手段１１は、これらの操作者ＩＤおよびパスワードを判定手段１２に与える。判定手段は与えられた操作者ＩＤおよびパスワードが一致しているか否か判断し、一致している場合には、一致判断信号を送受信手段１１に与える。なお、判別手段が、ＩＤおよびパスワードに換えて、操作者がデータ伝送機器の正当な使用者であることを判別するようにしてもよい。判別手法としては指紋、

声紋等を用いた判別が、採用可能である。

【００３６】送受信手段１１は、かかる一致判断信号を受けて、接続状態制御手段６にＶＰＮ伝送基礎データの読み出し許可信号を送信する。接続状態制御手段６はかかる読み出し許可信号を受け取ると、ＶＰＮ伝送基礎データ取得要求を送受信手段１１に出力する。送受信手段１１はＶＰＮ伝送基礎データをＶＰＮ伝送基礎データ記憶手段１０から読み出して、接続状態制御手段６に出力する。接続状態制御手段６は、与えられたＶＰＮ伝送基礎データを読み出しデータ記憶手段４に記憶させる。

【００３７】かかる読み出しデータ記憶手段４への書き込みにより、ＶＰＮサーバ１００との間でネットワークを介しても伝送対象データの守秘性を保持しつつ、データ伝送が可能となる。本明細書においては、かかる状態をＶＰＮが構築されたと呼ぶ。

【００３８】データ伝送について説明する。暗号化手段３は、処理手段２から暗号処理対象のデータを受け取ると、読み出しデータ記憶手段４に記憶されたＶＰＮ伝送基礎データのうちＶＰＮクライアント２００にて暗号化処理に用いるＶＰＮ暗号化キーを用いて暗号化し、ＶＰＮクライアント２００によって暗号化されたデータをＶＰＮサーバ１００が受信した場合に、これを復号化する時に用いるＶＰＮ復号化キーを特定するＶＰＮ復号化キー特定情報とともに、ＶＰＮサーバ１００のＩＰアドレスに転送する。

【００３９】ＶＰＮサーバ１００は、復号化手段１５，ＶＰＮ伝送基礎データ記憶手段１４，暗号化手段１３を備えている。復号化手段１５は、前記ＶＰＮ復号化キー特定情報に基づき、ＶＰＮ伝送基礎データ記憶手段１４に記憶された複数の復号化キーから復号処理に用いるキーを特定し、ＶＰＮクライアント２００によって暗号化されたデータを復号化して、他のコンピュータへ出力する。

【００４０】ＶＰＮ伝送基礎データ記憶手段１４は、ＶＰＮサーバ１００にて暗号化処理に用いるＶＰＮ暗号化キー、およびＶＰＮサーバ１００によって暗号化されたデータをＶＰＮクライアント２００が受信した場合に、これを復号化する時に用いるＶＰＮ復号化キーを特定するＶＰＮ復号化キー特定情報を含むＶＰＮ伝送基礎データを記憶する。暗号化手段１３は、ＶＰＮ伝送基礎データ記憶手段１４に記憶された暗号化キーを用いて、他のコンピュータから与えられたデータを暗号化して、ＶＰＮ伝送基礎データ記憶手段１４に記憶されたＶＰＮ復号化キー特定情報とともに、伝送データを受け取ったコンピュータのＩＰアドレス（この場合、ＶＰＮクライアント２００のＩＰアドレス）に転送する。

【００４１】ＶＰＮクライアント２００の復号化手段５は、ＶＰＮサーバ１００から受け取ったＶＰＮ復号化キー特定情報に基づき、読み出しデータ記憶手段４に記憶された復号化キーのうち復号処理に用いるキーを特定し、ＶＰＮサーバ１００によって暗号化されたデータを復号化して、処理手段２へ出力する。

【００４２】なお、上記例では、ＶＰＮクライアント２００からデータ伝送する場合について説明したが、ＶＰＮサーバ１００からデータ伝送することも可能である。この場合の処理は同様であるので説明は省略する。

【００４３】なお、ＶＰＮクライアントのＩＰアドレスについては、例えば、ＶＰＮクライアント２００からＶＰＮサーバ１００にデータが伝送された時に取得できる。

【００４４】また、ＶＰＮクライアントのＩＰアドレスを、予め、ＶＰＮサーバのＶＰＮ伝送基礎データ記憶手段に記憶しておくことにより、ＶＰＮサーバからのＶＰＮ伝送も可能である。

【００４５】また、ＶＰＮクライアントとしてユーザに選択されるコンピュータの範囲が決定されている場合には、ＶＰＮサーバにＶＰＮクライアントＩＰアドレスの候補を複数記憶しておいてもよい。この場合には、ＶＰＮサーバからＶＰＮを構築することも可能となる。

【００４６】また、上記実施形態においては、ＶＰＮ伝送基礎データとして、ＶＰＮ暗号化キー、ＶＰＮ復号化キー特定情報、およびＶＰＮサーバのＩＰアドレスを含む場合について説明したが、ＶＰＮ暗号化キーについては、ＶＰＮ暗号化キーを特定するためのＶＰＮ暗号化キー特定情報であってもよい。この場合、ＶＰＮ暗号化キーを特定するためのプログラムを記憶しておき、ＶＰＮクライアント単独でまたはＶＰＮサーバと連携してＶＰＮ暗号化キーを決定（生成）してもよい。

【００４７】また、ＶＰＮクライアントのＶＰＮ伝送基礎データとして、少なくともＶＰＮキー特定情報および対向するＶＰＮサーバのＩＰアドレスを記憶しておき、ＶＰＮサーバと連携してＶＰＮ暗号化キーおよびＶＰＮ復号化キーを決定するようにしてもよい。なお、ＶＰＮサーバのＶＰＮ伝送基礎データとして、少なくともＶＰＮキー特定情報および対向するＶＰＮクライアントのＩＰアドレスを記憶しておき、ＶＰＮクライアントと連携してＶＰＮ暗号化キーおよびＶＰＮ復号化キーを決定するようにしてもよい。

【００４８】かかるＶＰＮ暗号化キーおよびＶＰＮ復号化キーの生成については、例えば、IPSECの標準鍵交換方式のIKE（internet key exchange）を用いてもよい。

【００４９】このようにして、非閉鎖的なネットワークを介しても、守秘性の高いデータ伝送が可能となるＶＰＮが構築状態となる。

【００５０】２．ハードウェア構成

図２に示すＶＰＮサーバ１００のハードウェア構成について図３を用いて説明する。図３は、ＶＰＮサーバ１００をＣＰＵを用いて構成したハードウェア構成の一例である。以下では、ＶＰＮの標準プロトコルとして、IPSec(Security Architectuer for Internet Protocol)の鍵

交換方式の１つである手動鍵方式を採用した場合について説明する。

【００５１】ＶＰＮサーバ１００は、ＣＰＵ２３、メモリ２７、ハードディスク２６、ＣＲＴ３０、ＣＤＤ（ＣＤＲＯＭドライブ）２５、キーボード２８、マウス３１、ネットワーク管理部３２およびバスライン２９を備えている。ＣＰＵ２３は、ハードディスク２６に記憶されたプログラムにしたがいバスライン２９を介して、各部を制御する。なお、オペレーティングシステムとしては、例えば、ウインドウズＮＴ（商標）等を採用すればよい。

【００５２】ハードディスク２６には、オペレーティングプログラム（ＯＳ）２６ｏ、ＶＰＮサーバプログラム２６ｐ、およびＶＰＮデータ記憶部２６ｄを有する。

【００５３】これらのプログラムは、ＣＤＤ２５を介して、プログラムが記憶されたＣＤＲＯＭ２５ａから読み出されてハードディスク２６にインストールされたものである。なお、ＣＤＲＯＭ以外に、フレキシブルディスク（ＦＤ）、ＩＣカード等のプログラムをコンピュータ可読の記録媒体から、ハードディスクにインストールさせるようにしてもよい。さらに、通信回線を用いてダウンロードするようにしてもよい。

【００５４】本実施形態においては、プログラムをＣＤＲＯＭからハードディスク２６にインストールさせることにより、ＣＤＲＯＭに記憶させたプログラムを間接的にコンピュータに実行させるようにしている。しかし、これに限定されることなく、ＣＤＲＯＭに記憶させたプログラムをＣＤＤ２５から直接的に実行するようにしてもよい。なお、コンピュータによって、実行可能なプログラムとしては、そのままのインストールするだけで直接実行可能なものはもちろん、一旦他の形態等に変換が必要なもの（例えば、データ圧縮されているものを、解凍する等）、さらには、他のモジュール部分と組合して実行可能なものも含む。

【００５５】ＶＰＮデータ記憶部２６ｄのデータ構造について、図４を用いて説明する。ＶＰＮデータ記憶部２６ｄには、ＶＰＮクライアント識別子、ＶＰＮサーバ識別子、ＶＰＮ暗号化方式、ＶＰＮ復号化キー、およびＶＰＮ暗号化キーが記憶されている。

【００５６】ＶＰＮクライアント識別子およびＶＰＮサーバ識別子は、ＶＰＮサーバとＶＰＮクライアントとの間で暗号化されて伝送されるデータについて、いずれのデータを用いて復号すればよいかを決定するためのＶＰＮ復号化キー特定情報である。詳しくは後述する。ＶＰＮ復号化キーは、ＶＰＮクライアントにおいて暗号化されたデータをＶＰＮサーバにて復号するためのキーである。ＶＰＮ暗号化方式とは、ＶＰＮクライアントおよびＶＰＮサーバにおいて暗号化する暗号化方式を示すデータである。ＶＰＮ暗号化キーは、このＶＰＮクライアントに伝送する場合の暗号化キーである。

【００５７】たとえば、ＶＰＮクライアント識別子「ＡＣ１０１」、ＶＰＮサーバ識別子「ＡＳ１０５」、ＶＰＮ暗号化方式「ｘｘｘ１」、ＶＰＮ復号化キー「５９５ｘｘｘ５」、ＶＰＮ暗号化キー「３２５ｙｙｙ７」であれば、ＶＰＮクライアント識別子「ＡＣ１０１」からＶＰＮサーバ識別子「ＡＳ１０５」宛に伝送されたデータは、ＶＰＮ復号化キー「５９５ｘｘｘ５」を用いてＶＰＮ暗号化方式「ｘｘｘ１」で復号化される。また、ＶＰＮクライアント識別子「ＡＣ１０１」へのＶＰＮサーバ識別子「ＡＳ１０５」から伝送されるデータは、ＶＰＮ暗号化キー「３２５ｙｙｙ７」を用いてＶＰＮ暗号化方式「ｘｘｘ１」で暗号化される。

【００５８】このように、ＶＰＮサーバ１００には、ＶＰＮクライアントとの間でのＶＰＮ伝送方法を特定するデータが複数記憶されている。

【００５９】ネットワーク管理部３２はトラスト側（内部ＬＡＮ側）とアントラスト側（インターネット側）のデータを区別して送受信することができる。

【００６０】また、ＶＰＮプログラム２６ｐについては後述する。

【００６１】図２に示すＶＰＮクライアント２００のハードウェア構成について図５を用いて説明する。ＶＰＮクライアント２００は、ＶＰＮサーバ１００とハードウェア構成はほぼ同じであるが、さらにＵＳＢＩＦ１３３を有している。ＵＳＢＩＦ１３３は、ＵＳＢ(universal serial bus）のインターフェイスである。また、ハードディスク１２６に記憶されているデータが異なり、ＶＰＮクライアントプログラム１２６ｓおよびアプリケーションプログラム１２６ａを有する。

【００６２】各プログラムについては後述する。

【００６３】図２に示すデータ伝送機器３００のハードウェア構成について図６を用いて説明する。データ伝送機器３００は、ＣＰＵ２２３，ＲＯＭ２２５、フラッシュメモリ２２７、パスワード判定部２３３、ＵＳＢＩＦ２３２およびバスライン２２９を備えている。本実施形態においては、データ伝送機器３００としてＶＰＮクライアント２００に設けられたＵＳＢ端子（図示せず）にＵＳＢプラグを挿入することにより、ＶＰＮクライアント２００との間で内部に有するデータをデータ伝送可能なＵＳＢ機器（ＵＳＢキー）を採用した。ＲＯＭ２２５には外部との通信および各部を制御する制御プログラムが記録されている。フラッシュメモリ２２７には、ＶＰＮデータ記憶領域２２８を有している。ＶＰＮデータ記憶領域２２８について、図７を用いて説明する。ＶＰＮデータ記憶領域２２８には、ユーザＩＤ、パスワード、使用期限、ＶＰＮサーバのＩＰアドレス、相手先サーバのＩＰアドレス、ＶＰＮ暗号化方式、ＶＰＮ暗号化キー、ＶＰＮ復号化キー、ＶＰＮクライアント識別子、およびＶＰＮサーバ識別子が記憶されている。相手先サーバは例えば、ウェブサーバを示す。

【００６４】ユーザＩＤおよびパスワードは、このデータ伝送機器３００を使用許可が与えられているユーザであることを判別するためのデータである。使用期限は、このデータ伝送機器３００を使用できる期限を表す。ＶＰＮサーバのＩＰアドレスは、ＶＰＮ暗号化方式およびＶＰＮ暗号化キーによって、暗号化したデータを転送先であり、相手先サーバのＩＰアドレスは、ＶＰＮサーバによって復号化されたデータの転送先を示す。ＶＰＮ復号化キーは、ＶＰＮサーバから与えられた暗号化されたデータを復号化する場合のキーである。ＶＰＮクライアント識別子およびＶＰＮサーバ識別子は、ＶＰＮサーバとの間で相対的に決定された２つのコンピュータの識別子である。この点は、ＶＰＮサーバと同様である。

【００６５】パスワード判定部２３３は与えられたＩＤおよびパスワードがあらかじめ記憶されているＩＤおよびパスワードと一致するか否かをハードウェアロジックで判断し、一致する場合には一致判断信号を出力し、一致しない場合には不一致判断信号を出力する。

【００６６】３．フローチャート

以下では、既に述べたように、ＶＰＮの標準プロトコルとして、IPSecの鍵交換方式の１つである手動鍵方式を採用した場合について説明する。

【００６７】図８～図１１を用いて、ＶＰＮサーバ１００とＶＰＮクライアント２００におけるＶＰＮを用いたデータ伝送処理について説明する。以下では、図５に示すようなアプリケーションプログラム２６ａに基づいて出力されたデータを、ＶＰＮサーバ１００に暗号化したまま送信し、図１に示すＶＰＮサーバ１００にＬＡＮ接続されたウェブサーバ１１０に復号化したデータとして転送する場合を例として説明する。

【００６８】まず、図８を用いてＶＰＮの構築処理について説明する。データ伝送機器３００とＶＰＮクライアント２００との間で、以下のようにして、ＶＰＮ基礎データが読み出され、メモリ１２７に書き込まれる。

【００６９】まず、ユーザはデータ伝送機器３００をＶＰＮクライアント２００のＵＳＢ端子に挿入する。ＶＰＮクライアント２００は、ＯＳ１２６ｏに基づいて、自己のＵＳＢ端子（図示せず）にデータ伝送機器３００が挿入されるか否かを検出しており、挿入を検出すると、使用期限内か否か判断し、使用期限内であれば、当該ユーザがデータ伝送機器３００の使用を許可されたユーザであるか否かを判断するために、ユーザＩＤおよびパスワードの入力画面を表示する（図８ステップＳ１）。ユーザは、キーボード１２８からユーザＩＤおよびパスワードを入力する。

【００７０】ＣＰＵ１２３は、ユーザＩＤおよびパスワードの入力があるか否か判断しており（ステップＳ３）、ユーザＩＤおよびパスワードの入力があると、データ伝送機器３００へ入力されたユーザＩＤおよびパスワードをＵＳＢＩＦ１３２を介して送信する（ステップＳ５）。

【００７１】データ伝送機器３００のＣＰＵ２２３は、ＵＳＢＩＦ２３２を介してユーザＩＤおよびパスワードを受信するか否か判断しており（ステップＳ２１）、かかるデータを受信すると、パスワード判定部２３３（図６参照）に受信したユーザＩＤおよびパスワードを与える（ステップＳ２３）。パスワード判定部２３３は、既に説明したように、入力されたユーザＩＤおよびパスワードと、予め記録されているユーザＩＤおよびパスワードとが一致する場合には、一致信号を出力し、一致しない場合には、不一致信号を出力する。ＣＰＵ２２３は、パスワード判定部２３３から一致信号が与えられるか否か判断しており（ステップＳ２５）、一致信号が与えられるとＶＰＮクライアント２００にＵＳＢＩＦ２３２を介して一致信号を送信する（ステップＳ２７）。

【００７２】ＶＰＮクライアント２００のＣＰＵ１２３は、ＵＳＢＩＦ１３２を介して一致信号を受信するか否か判断しており（ステップＳ７）、一致信号を受信するとデータ伝送機器３００に記憶されたＶＰＮ伝送基礎データを取得するための要求命令を、ＵＳＢＩＦ１３２を介してデータ伝送機器３００に送信する（ステップＳ９）。

【００７３】データ伝送機器３００のＣＰＵ２２３は、ＵＳＢＩＦ２３２を介して前記要求命令が与えられるか否か判断しており（ステップＳ３１）、前記要求命令が与えられると、ＶＰＮデータ記憶領域に記憶されたデータを、ＵＳＢＩＦ２３２を介して、ＶＰＮクライアント２００に送信する（ステップＳ３３）。

【００７４】ＶＰＮクライアント２００のＣＰＵ１２３は、応答があるか否か判断しており（ステップＳ１１）、応答があるとメモリ１２７に受信したＶＰＮ伝送基礎データを書き込む（ステップＳ１３）。

【００７５】かかるＶＰＮ伝送基礎データのメモリ１２７への書き込みにより、後述するようにＶＰＮを用いた伝送が可能な状態となる。本明細書では、これを、ＶＰＮが構築されたと呼ぶ。

【００７６】なお、ステップＳ２５にて、不一致信号を受け取ると、ＣＰＵ２２３は、ＵＳＢＩＦ２３２を介してＶＰＮクライアント２００に不一致信号を送信する（ステップＳ３５）。クライアント２００のＣＰＵ１２３は、ステップＳ７にて不一致信号を受信し、例えば、「ユーザＩＤまたはパスワードが違います。正しいユーザＩＤおよびパスワードを入力してください。」とアラームメッセージを表示する（ステップＳ１５）。そして、ステップＳ１以下の処理を繰り返す。

【００７７】ＶＰＮクライアント２００とＶＰＮサーバ１００との間の伝送処理は、従来のＶＰＮを用いた伝送と基本的には同じである。以下、図９を用いて、ＶＰＮを用いた伝送処理について説明する。

【００７８】ＶＰＮクライアント２００のＣＰＵ１２３

は、伝送対象のパケットのヘッダに記載された、伝送先コンピュータのＩＰアドレスを参照して、内部から外部への送信要求があるか否か判断する（図９ステップＳ４１）。この場合、アプリケーションプログラム２６ａに基づいて出力されたデータを、図１に示すウェブサーバ１１０に伝送する場合であるので、伝送対象のパケットのヘッダに記載されたウェブサーバ１１０のＩＰアドレスを参照して、かかる判断を実行する。

【００７９】つぎに、ＣＰＵ１２３は、送信先がＶＰＮを用いた伝送を実行する送信先か否かを判断する（ステップＳ４３）。これは、伝送対象パケットのヘッダ情報を参照して、伝送先コンピュータのＩＰアドレスが、メモリ１２７に読み出されているＶＰＮ伝送基礎データの相手先サーバのＩＰアドレスと一致するか否かを判断すればよい。

【００８０】一致する場合は、ＣＰＵ１２３は、ＶＰＮ伝送基礎データを用いて暗号化して送信する（ステップＳ４５）。具体的には、伝送対象のパケットをＶＰＮ暗号化キーを用いてＶＰＮ暗号化方式で暗号化し、パケット化する。このパケットのヘッダにこのパケットの伝送先であるＶＰＮサーバのＩＰアドレス、ＶＰＮクライアント識別子、およびＶＰＮサーバ識別子をヘッダに埋め込んで、送信する。なお、通常の送信と同様に、送信元であるＶＰＮクライアント２００のＩＰアドレスもヘッダに埋め込まれる。一方、ステップＳ４３にて、一致しない場合は、ＶＰＮを用いた伝送ではないので、伝送対象パケットを破棄する（ステップＳ４７）。なお、指定されたＩＰアドレスのコンピュータに暗号化することなく送信するようにしてもよい。この場合、ステップＳ４５にて暗号化することなく、送信するようにすればよい。

【００８１】ＶＰＮサーバ１００のＣＰＵ２３は、外部から内部への要求（リクエスト）を受信したか否か判断している（ステップＳ６１）。なお、外部からの要求であるか否かは、ネットワーク管理部のアントラスト側へ与えられたか否かを判断すればよい。内部への要求であるかは、伝送パケットのヘッダに自己のＩＰアドレスが転送先として指定されているか否か等を判断すればよい。

【００８２】外部から内部への要求を受信すると、ＣＰＵ２３は、指定先が図４に示すＶＰＮデータ記憶部のデータリスト中に存在するか否かを判断する（ステップＳ６３）。具体的には、ヘッダに存在するＶＰＮクライアント識別子およびＶＰＮサーバ識別子を検索キーとして、リストに存在するか否かを判断する。この場合、リストに存在するので、ヘッダ中から送信元であるＶＰＮクライアント２００のＩＰアドレスを読み出して、直前ＶＰＮクライアントＩＰアドレスをそのＩＰアドレスに書き換える（ステップＳ６４）。この場合、ヘッダ情報として、ＶＰＮクライアント識別子「ＡＣ１０１」およびＶＰＮサーバ識別子「ＡＳ１０５」が読み出され、図４に示すリストに存在するので、送信元のＶＰＮクライアント２００のＩＰアドレスを直前ＶＰＮクライアントＩＰアドレスに書き換える。このように、ＶＰＮ復号化キー特定情報に対応づけてＶＰＮクライアントＩＰアドレスを記憶しておくことにより、ＶＰＮクライアントＩＰアドレスが動的に変化する場合でも、ＶＰＮを用いたデータ通信が可能となる。

【００８３】ＣＰＵ２３は、ＶＰＮ復号化キーを特定して暗号化方式に則って復号化し、復号化後のデータから、転送先のサーバのＩＰアドレスを抽出し、当該ＩＰアドレスのサーバに転送する（ステップＳ６５）。この場合、対応するＶＰＮ復号化キー「５９５ｘｘｘ５」を用いて、ＶＰＮ暗号化方式で復号化する。復号化後のデータのヘッダ情報を参照すると、このパケットの相手先サーバのＩＰアドレスが、「２０２．ｘｘｘ．ｘｘｘ」であることがわかるので、かかるコンピュータに復号化したパケットを伝送する。

【００８４】このように、ヘッダ情報に埋め込まれたＶＰＮクライアント識別子およびＶＰＮサーバ識別子は、ＶＰＮサーバ１００にて伝送されたパケットを復号化する場合の復号化キーを特定するデータとして機能する。

【００８５】伝送先のウェブサーバ１１０でデータ処理が実行されて、ＶＰＮクライアント２００に応答を伝送する場合、次のように実行される。

【００８６】ＶＰＮサーバ１００のＣＰＵ２３は、内部から外部への要求を受信したか否か判断している（ステップＳ７１）。なお、内部からの要求であるか否かは、ネットワーク管理部のトラスト側へ与えられたか否かを判断すればよい。したがって、ウェブサーバ１１０からＶＰＮクライアント２００への伝送データを受け取ると、送信先がＶＰＮリストに存在するか否か判断する（ステップＳ７３）。この場合、この伝送データの送信先として、ウェブサーバ１１０は、自己が受信した要求発信元として指定されたＩＰアドレスが、直前ＶＰＮクライアントＩＰアドレスとして記憶されているか否か判断すればよい。

【００８７】この場合、送信先がＶＰＮリストに存在するので、該当するＶＰＮ暗号化キー、ＶＰＮ暗号化方式を用いて、暗号化して、直前ＶＰＮクライアントＩＰアドレスに送信する（ステップＳ７５）。このとき、ヘッダ情報に、ＶＰＮクライアント識別子およびＶＰＮサーバ識別子を埋め込む。かかるデータを埋め込むのは、ＶＰＮクライアント２００にて伝送されたパケットを復号化する場合の復号化キー特定するためである。なお、ステップＳ７５にて暗号化することなく、送信するようにしてもよい。

【００８８】ＶＰＮクライアント２００のＣＰＵ１２３は、外部から内部への要求（リクエスト）を受信したか否か判断している（ステップＳ５１）。これは、伝送対

象パケットのヘッダ情報に記憶された送信元のＶＰＮサーバのＩＰアドレスおよび送信先のＶＰＮクライアントのＩＰアドレスから判断すればよい。

【００８９】ＣＰＵ１２３は、メモリ１２７に読み出しているＶＰＮ伝送基礎データで復号すべきか否かを判断する（ステップＳ５３）。具体的には、伝送対象パケットのヘッダ情報に存在するＶＰＮクライアント識別子およびＶＰＮサーバ識別子が、メモリ１２７に読み出しているＶＰＮ伝送基礎データのＶＰＮクライアント識別子およびＶＰＮサーバ識別子と一致するか否かを判断すればよい。

【００９０】この場合、一致するので、メモリ１２７に読み出しているＶＰＮ伝送基礎データのＶＰＮ復号化キーを用いて、復号化し、アプリケーションプログラムに渡す（ステップＳ５５）。以下、かかる処理を繰り返す。

【００９１】なお、ステップＳ５３にて一致しない場合には、ＶＰＮを用いた伝送ではないので破棄する（ステップＳ５７）。なお、ステップＳ７５にて暗号化されないで送信された場合には、ステップＳ５５にて、復号化することなくアプリケーションプログラムに渡すようにすればよい。

【００９２】本実施形態においては、ＶＰＮクライアントのＩＰアドレスが固定的ではない。したがって、図９ステップＳ６４において、図４に示すリストに存在する場合には、直前ＶＰＮクライアントＩＰアドレスとして記憶するようにしている。これにより、ＶＰＮクライアントのＩＰアドレスに拘束されず、自由にＶＰＮを構築することができる。また、ＶＰＮクライアント２００にて、データ伝送機器３００が取り外された場合には、ＶＰＮクライアント２００のメモリから、読み出されたＶＰＮ伝送基礎データを消去するだけで、ＶＰＮサーバにはデータ伝送機器３００が取り外されたことを送信しない。この場合でも、つぎに、同じまたは異なるコンピュータをＶＰＮクライアントとしてＶＰＮ伝送がなされると、動的に前記ＶＰＮクライアントのＩＰアドレスを記憶するので、確実に、ＶＰＮクライアントのＩＰアドレスに拘束されないＶＰＮを構築することができる。

【００９３】なお、図９ステップＳ７３にて、リストに存在しない場合は、ＶＰＮを用いた伝送ではないので破棄（無視）する（ステップＳ７７）。

【００９４】ＶＰＮ切断処理について図１０を用いて説明する。ＶＰＮクライアント２００のＣＰＵ１２３は、ＯＳ１２６ｏに基づき、ＵＳＢ端子の接続状態が変化するか否かを判断している。ＶＰＮクライアント２００のＣＰＵ１２３は、図１０に示すプログラムを実行しており、「ＵＳＢ端子からデータ伝送機器が取り外された」との検出結果を受けるか否かを判断しており（ステップＳ８１）、ＵＳＢ端子からデータ伝送機器３００が取り外されると、メモリ１２７のＶＰＮ伝送基礎データを消去する（ステップＳ８３）。これにより、ＶＰＮ伝送が不可能な状態となる。これを、ＶＰＮ切断状態という。

【００９５】このように、ＶＰＮ伝送基礎データを携帯可能な接続機器に記録しておき、必要な端末に挿入することにより、コンピュータのＩＰアドレスに拘束されないＶＰＮを構築することができる。また、接続機器を取り外すことにより、自動的にＶＰＮ伝送基礎データが消去されるので、当該コンピュータにて第三者がこのＶＰＮを用いた伝送をすることを確実に防止することができる。

【００９６】４．他の実施形態

なお、本実施形態においては、伝送機器としてＵＳＢキーを用いたが、クライアントコンピュータとの間で内部に記憶されているデータのやりとりができるものであればどのようなものであってもよく、コンパクトフラッシュ（登録商標）、ＰＣカード等の記録媒体を採用してもよい。また、コンピュータに設けられた端子に有線で接続する場合だけでなく、赤外線データ通信（例えば、IrDA（Infrared Data Association）規格など）やBluetoothなどで接続することも可能である。

【００９７】また、データ伝送機器の発行および記録データの変更については、別途発行処理管理コンピュータを設ければよい。また、ＩＤおよびパスワードを入力することにより、ＶＰＮクライアントで編集可能としてもよい。

【００９８】なお、ＲＳＡなどの公開鍵形式で暗号化および復号化をする場合には、ＶＰＮサーバ１００の公開鍵については、データ伝送機器３００のＶＰＮ伝送基礎データ記憶手段１０に記憶しておく必要はなく、暗号化するときに、ＶＰＮサーバ１００にアクセスして取得するようにしてもよい。ＶＰＮクライアント２００の公開鍵についても同様である。

【００９９】本実施形態においては、ＶＰＮ伝送基礎データを全てデータ伝送機器に格納して持ち歩くようにしている。これにより、ＶＰＮサーバからＶＰＮ伝送基礎データを転送させる必要がないので、守秘性を高めることができる。しかし、ＶＰＮ伝送基礎データを全てデータ伝送機器に格納させるのではなく、その一部を格納させておき、残りのデータはＶＰＮサーバからダウンロードするようにしてもよい。この場合、データの分割の仕方としては、合体させて初めてデータとして意義があるように、分割すればよい。たとえば、ＶＰＮ暗号キーが１２バイトから構成されている場合、前半の６バイトをデータ伝送機器に、後半の６バイトをＶＰＮサーバから転送させて、両者を合体させて初めてＶＰＮ暗号キーがわかるようにすればよい。他の項目データについても同様である。この場合、分割の割合については、限定されない。

【０１００】また、上記実施形態においては、図５に示すように、ＶＰＮクライアント１１のハードディスクに

ＶＰＮプログラム１２６ｃをインストールしている場合について説明したが、ＶＰＮプログラムについては、フラッシュメモリチップおよびコントローラチップを搭載したコンパクトフラッシュ（CF)等の記録媒体に格納し、かかる記録媒体からプログラムを読み出すようにしてもよい。これにより、ＶＰＮプログラムを予めインストールしていないコンピュータであっても、ＶＰＮ通信が可能となる。以下、図５に示すＶＰＮクライアントで記述しているＶＰＮプログラムをデータ伝送機器に内蔵した場合の実施形態について、説明する。

【０１０１】図１１に、ＶＰＮクライアントとしてＰＤＡ（Personal Digital Assistants）を採用した場合の、ハードウェア構成を示す。このように、ＰＤＡ４００はＣＦスロット４３３を有しており、ＣＦスロット４３３には後述するコンパクトフラッシュ４３３ａが挿入される。ＲＯＭ４２５にはオペレーティングシステムプログラム（ＯＳ）が記憶されている。

【０１０２】コンパクトフラッシュ４３３ａのデータ構造を図１２を用いて説明する。コンパクトフラッシュ４３３ａは、ＰＤＡ４００のＣＰＵ４２３がＯＳによって認識できる領域と、認識できない領域に分割されている。これにより、ＶＰＮ個人情報等のＶＰＮ伝送基礎データの無断複製等から保護することができる。

【０１０３】図１２に示すように、コンパクトフラッシュ４００は、ＰＤＡ４００のＯＳが認識できる領域４１１と、ＰＤＡ４００のＯＳが認識できない領域４１２にパーティションが分けられている。具体的には領域４１１はＦＡＴが存在するが、領域４１２はhiddenFATとしてパーティションを分割すればよい。領域４１２に図６に示すＶＰＮデータ４１２ｄおよびこれを用いてＶＰＮサーバとの間でＶＰＮ通信を行うＶＰＮプログラム４１２ｖを、予め定めたデータフォーマットで記録しておく。領域４１２はＰＤＡ４００のＯＳが通常のファイルシステムのデータフォーマットとは異なるデータフォーマットで記憶されているので、領域４１１にこの領域４１２に記録されたプログラムを起動する起動プログラム４１２ａが記録されている。

【０１０４】かかる起動プログラム４１１ａおよびＶＰＮプログラム４１２ｖによるデータ処理を図１３を用いて説明する。

【０１０５】まず操作者は、コンパクトフラッシュ４３３ａをＣＦスロット４３３に挿入する。ＣＰＵ４２３は、ＲＯＭ４２５に格納されたＯＳに基づいてＣＦスロット４３３にコンパクトフラッシュが挿入されたか否かを判断しており（図１３ステップＳ１０１）、挿入があるとコンパクトフラッシュ４３３ａに自動実行のための定義ファイルを読み出す（ステップＳ１０５）。この場合、図１２に示すように、定義ファイル４１１ｂをコンパクトフラッシュから読み出す。定義ファイル４１１ｂには、領域４１１に記憶された起動プログラム４１１ａを実行する命令が記載されており（図示せず）、ＣＰＵ４２３は、起動プログラム４１１ａをＲＡＭ４２７にロードする（ステップＳ１０７）。これにより、起動プログラム４１１ａによる処理が実行される。

【０１０６】ＣＰＵ４２３は起動プログラム４１１ａに基づき、パスワード入力画面を液晶表示部４３０に表示する（ステップＳ１０９）。かかる表示がなされると、操作者はパスワードを入力部４２８から入力する。ＣＰＵ４２３はパスワード入力があったか否か判断しており（ステップＳ１１１）、パスワード入力があると、領域４１２に記憶されているＶＰＮプログラム４１２ｖを読み出す（ステップＳ１１５）。領域４１２は、既に説明したように、ＰＤＡ４００のＣＰＵ４２３のＯＳのファイル管理システムとは異なる形式でデータ記録されているため、ＯＳだけではデータを読み出すことはできない。しかし、起動プログラム４１１ａは予め領域４１２に記憶されたデータが読み出すための情報を記憶しているのでかかる情報を用いて、ＶＰＮプログラム４１２ｖを読み出すことができる。ＣＰＵ４２３は前記パスワードを用いて読みだしたＶＰＮプログラム４１２ｖを復号化する（ステップＳ１１７）。ＣＰＵ４２３は復号結果を参照して、復号ができるか否か判断しており（ステップＳ１１９）、復号ができたと判断した場合には、復号化したＶＰＮプログラム４１２ｖをＲＡＭ４２７にロードする（ステップＳ１２０）。なお、復号ができたか否かは、例えば、所定の位置に埋め込んでいた判断コードが復号化によって、読みとれるか否か判断するようにすればよい。これにより、ＶＰＮプログラム４１２ｖによる処理が実行される。

【０１０７】ＣＰＵ４２３は、ＶＰＮプログラム４１２ｖに基づき、ＶＰＮデータ４１２ｄを読み出す（ステップＳ１２１）。ＶＰＮデータ４１２ｄの読み出しについてはＶＰＮプログラム４１２ｖの場合と同様である。ＣＰＵ４２３は前記パスワードを用いて、読みだしたＶＰＮデータ４１２ｄを復号化する（ステップＳ１２３）。ＣＰＵ４２３は復号結果を参照して、復号できるか否か判断しており（ステップＳ１２５）、復号できたと判断した場合には、復号化したＶＰＮデータ４１２ｄをＲＡＭ４２７を用いて、ＶＰＮサーバとの間でＶＰＮを構築する（ステップＳ１２７）。これ以降は、上記実施形態と同様に、図９に示す伝送処理が実行される。

【０１０８】なお、ステップＳ１１９にて、復号化ができない場合には、「正しいパスワードを入力してください」等のエラーメッセージを、表示してステップＳ１０９以下の処理を繰り返す。

【０１０９】また、ステップＳ１２５にて、復号化ができない場合には、「データが壊れているおそれがあります。管理者に連絡してください」等のエラーメッセージを表示して（ステップＳ１２８）、処理を終了する。

【０１１０】なお、上記実施形態と同様に、ＰＤＡ４０

０のＣＰＵ４２３は、ＯＳに基づいて、ＣＦスロット４３３に挿入されたコンパクトフラッシュ４３３aが取り外されたか否かを判断しており（図１０に示す処理と同様に処理）、取り外されると、ＲＡＭ４２７にロードされたプログラムおよびＶＰＮデータを消去する。これにより、コンパクトフラッシュ４３３aをとり外した後は、当該ＰＤＡから許可なくＶＰＮを構築されるおそれがない。

【０１１１】このようにコンパクトフラッシュを用いることにより、ＵＳＢ端子を有しないＰＤＡ機器をＶＰＮクライアントとしてＶＰＮを構築することができる。なお、ＯＳの異なるコンピュータでもＶＰＮクライアントとして構築できるように、領域４１１をさらに複数に分けてそれぞれに同じ起動プログラムを記憶しておき、いずれかの領域から起動プログラムが読み出されることにより、ＶＰＮプログラムが起動できるようにすればよい。例えば、コンパクトフラッシュの領域４１１$_1$には、Ｐａｌｍ（商標）用ＯＳ、領域４１１$_2$には、windows（商標）ＣＥ用ＯＳ、領域４１１$_3$には、・・・というように記憶しておけばよい。

【０１１２】また、この例では、ＰＤＡをＶＰＮクライアントとする場合について説明したが、その他ノートパソコンなどの携帯端末についても同様に適用できる。

【０１１３】なお、かかる携帯端末が一旦記憶したデータをハードディスク等の記録媒体に一旦記憶するような場合には、前記読み出されたＶＰＮプログラムやＶＰＮデータをメモリ上だけでなく、かかる記録媒体から消去するプログラムを前記ＣＦ等に記憶させておき、自動実行するようにすればよい。

【０１１４】なお、図１３においては、コンパクトフラッシュがＣＦスロットに挿入されると、定義ファイルから起動プログラム４１１ａを自動実行する場合について説明したが、操作者が起動プログラム４１１ａを手動で実行することもできる。この場合、図１３において、ステップＳ１０１，ステップＳ１０５の代わりに、起動プログラムの実行指令が与えられたか否かで判断すればよい。

【０１１５】なお、図７に示すＶＰＮ伝送基礎データにて、相手先サーバのＩＰアドレスに代えて、ＩＰサブネットアドレスで指定するようにしてもよい。この場合、図９ステップＳ４３にて、伝送先コンピュータのＩＰアドレスが、メモリ１２７に読み出されているＶＰＮ伝送基礎データの相手先サーバの属するＩＰサブネットアドレスと一致するか否かを判断すればよい。すなわち、その他ドメイン名などの相手先サーバを一意に特定できる相手先サーバ特定情報を用いることができる。

【０１１６】本実施形態においては、ＶＰＮサーバとＶＰＮクライアントとの間のネットワークとして、インターネットを採用したが、これに限定されず、他のネットワークであっても、他のユーザに対する守秘性を保持できるという効果を奏する。

【０１１７】なお、記録媒体には、ＶＰＮ基礎データを読み出すＶＰＮ処理プログラムを記録しない場合でも、ＶＰＮ基礎データを前記領域４１２のようにＶＰＮクライアントのＯＳが認識できない領域に格納するようにしてもよい。この場合、かかる読み出すためのプログラムは予めＶＰＮクライアントに記憶しておけばよい。

【０１１８】また、本実施形態においては、通信プロトコルとしてＴＣＰ／ＩＰを採用したが、他の通信プロトコルを採用してもよい。

【０１１９】本実施形態においては、図２に示す機能を実現する為に、ＣＰＵを用い、ソフトウェアによってこれを実現している。しかし、その一部もしくは全てを、ロジック回路等のハードウェアによって実現してもよい。

【０１２０】なお、プログラムの一部の処理をさらに、オペレーティングシステム（ＯＳ）にさせるようにしてもよい。

【図面の簡単な説明】

【図１】本発明にかかるＶＰＮ伝送システムの概略を示す。

【図２】本発明にかかるＶＰＮ伝送システムの機能ブロック図である。

【図３】図２に示すＶＰＮサーバ１００をＣＰＵを用いて実現したハードウエア構成の一例を示す図である。

【図４】ＶＰＮ伝送基礎データのデータ構造を示す。

【図５】図２に示すＶＰＮクライアント２００をＣＰＵを用いて実現したハードウエア構成の一例を示す図である。

【図６】図１に示すデータ伝送機器３００をＣＰＵを用いて実現したハードウエア構成の一例を示す図である。

【図７】ＶＰＮ伝送基礎データのデータ構造を示す。

【図８】ＶＰＮ構築処理を示すフローチャートである。

【図９】ＶＰＮ伝送処理を示すフローチャートである。

【図１０】ＶＰＮ切断処理を示すフローチャートである。

【図１１】ＰＤＡをＶＰＮクライアントとする場合の、ＰＤＡのハードウエア構成の一例を示す図である。

【図１２】コンパクトフラッシュ４３３aのデータ管理方法を説明するための図である。

【図１３】ＶＰＮデータ読み出し処理を示すフローチャートである。

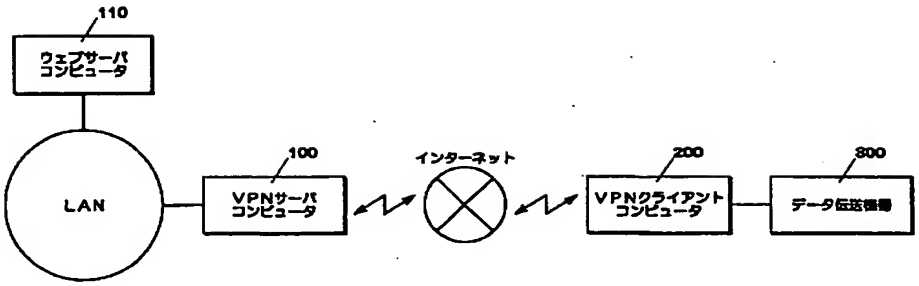
【図１４】従来のＶＰＮシステムの概要を示す図である。

【符号の説明】

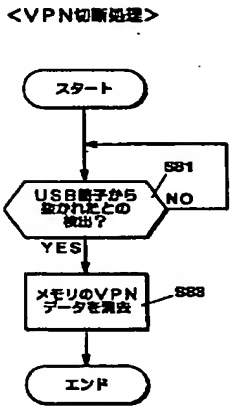
２３・・・ＣＰＵ
２７・・・メモリ
１００・・・ＶＰＮサーバ
１２３・・・ＣＰＵ
１２７・・・メモリ

２００・・・ＶＰＮクライアント
２２３・・・ＣＰＵ
２２７・・・メモリ
３００・・・データ接続機器

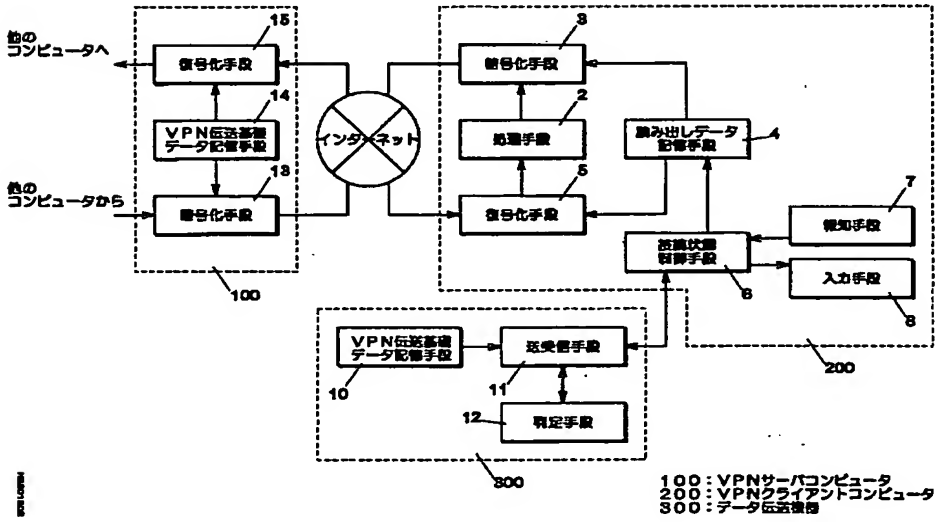
【図１】



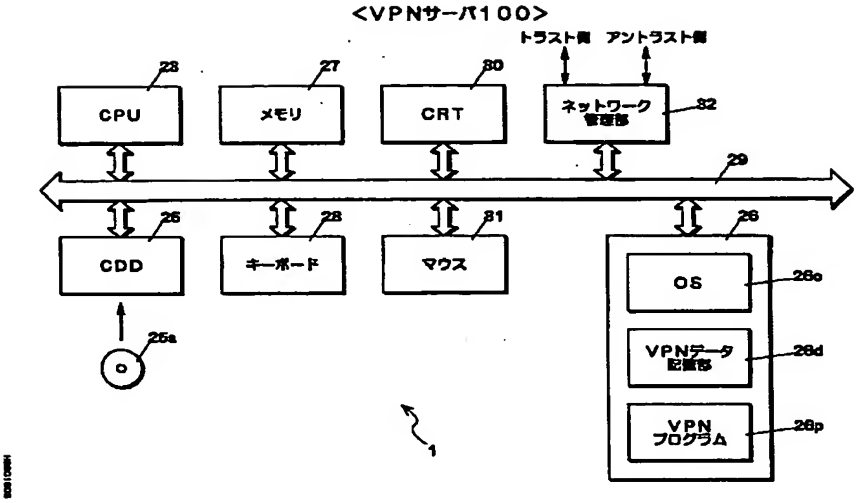
【図１０】



【図２】



【図３】

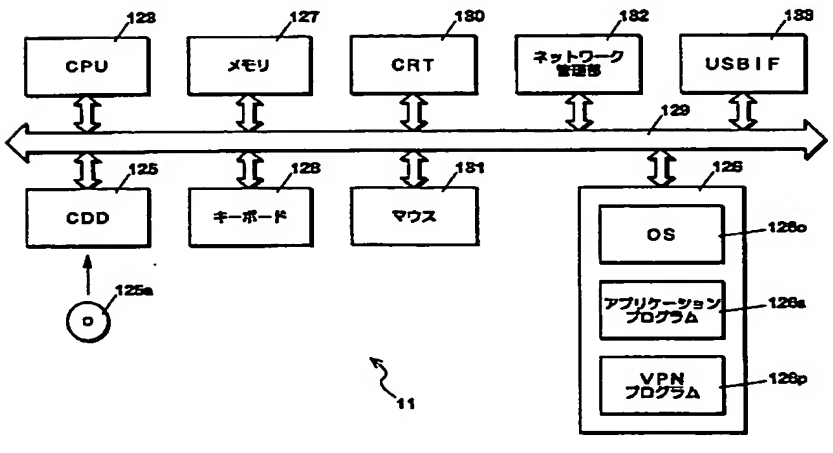


【図４】

<VPNデータ記憶部>

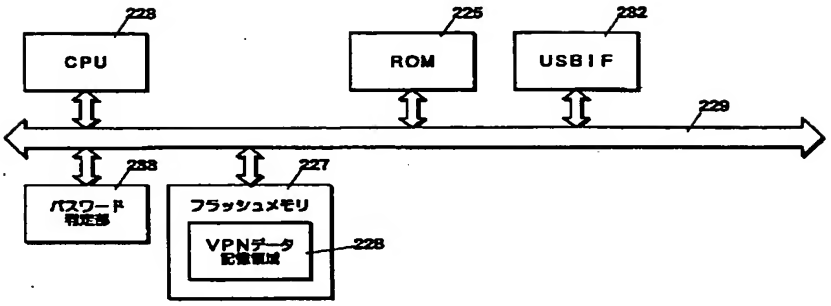
VPNクライアント識別子	VPNサーバ識別子	VPN暗号化方式	VPN復号化キー	VPN暗号化キー	割当VPNクライアントIPアドレス
AC101	AS105	XXX1	595XXX5	325YYY7	△△△
KC203	KS109	XXX2	305XXX3	936YYY2	
PC301	PS203	XXX1	408XXX7	556YYY1	
⋮	⋮	⋮	⋮	⋮	⋮

【図５】



【図６】

<データ伝送管理300>



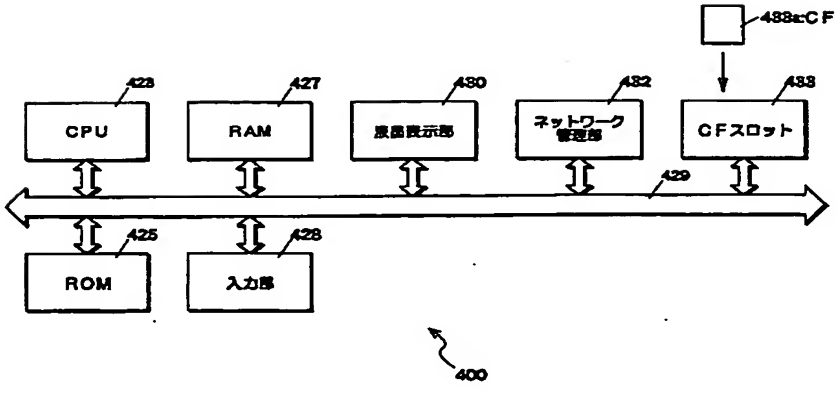
【図７】

<VPNデータ記憶領域>

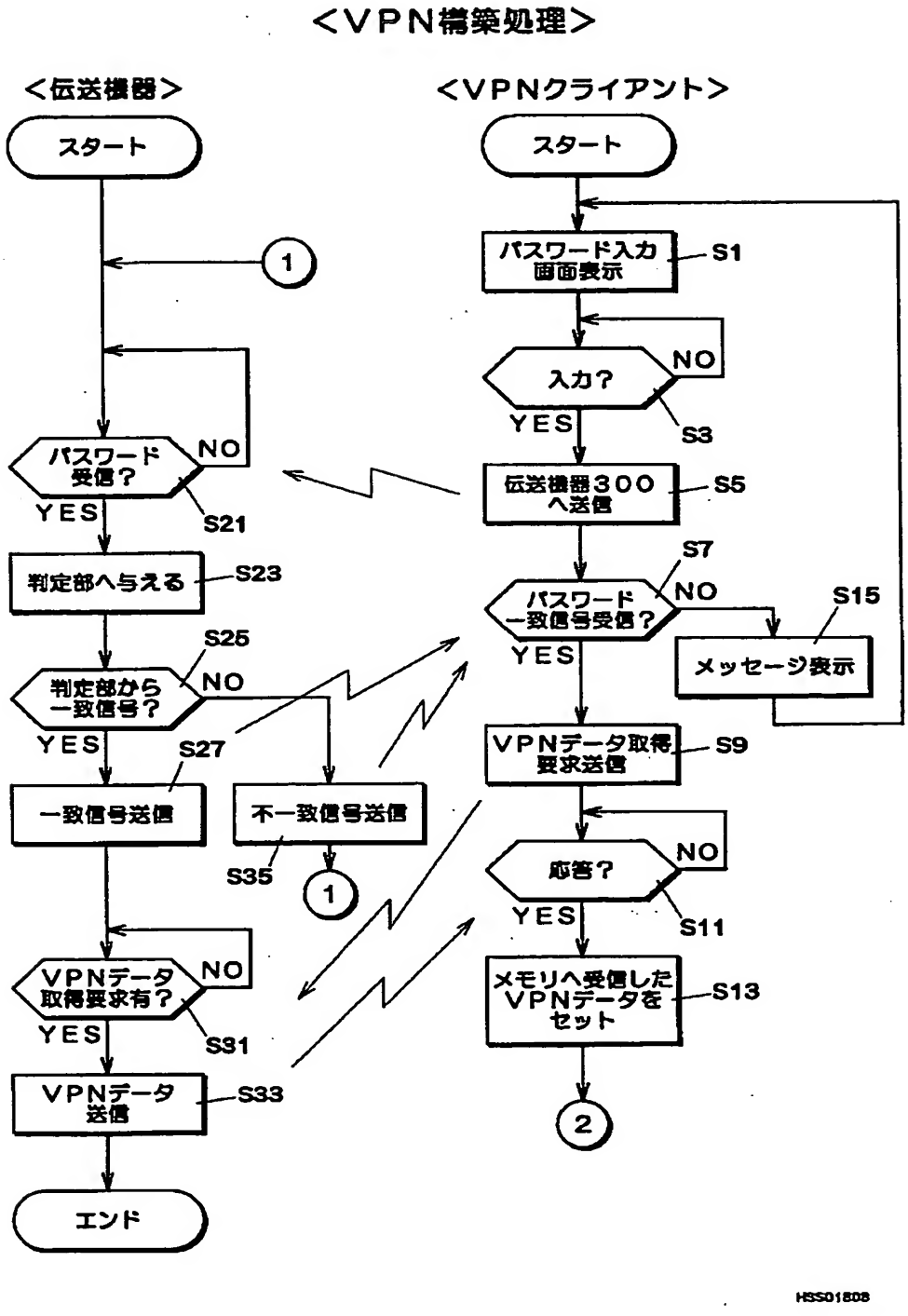
ユーザＩＤ	XX501
パスワード	*185018
使用期限	2001/12/31
VPNサーバのＩＰアドレス	202. XXX. YYY
相手先サーバのＩＰアドレス	202. XXX. XXX
VPN暗号化方式	XXX1
VPN暗号化キー	595XXX5
VPN復号化キー	325YYY7
VPNクライアント識別子	AC101
VPNサーバ識別子	AS105

【図１１】

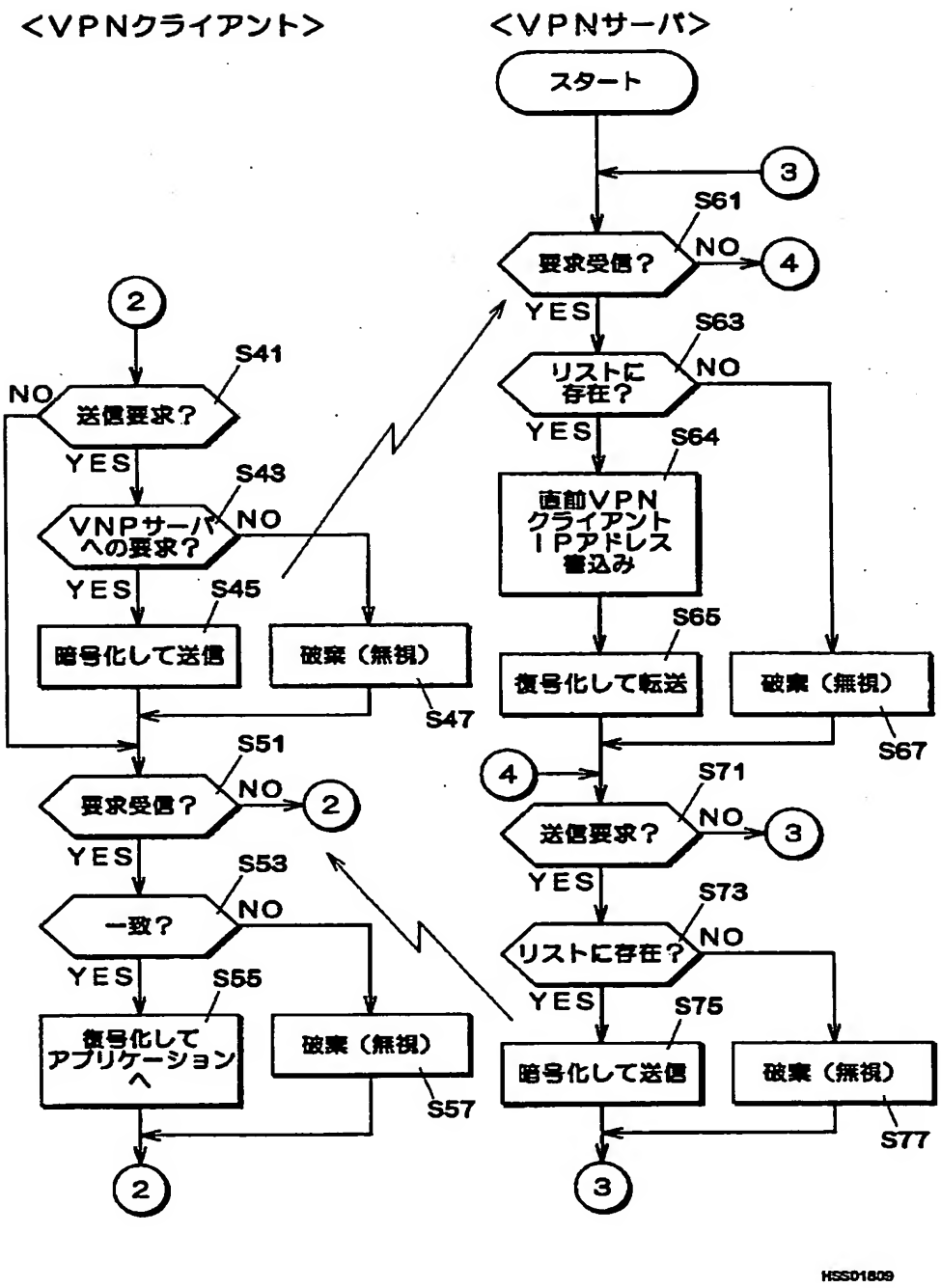
<PDA>



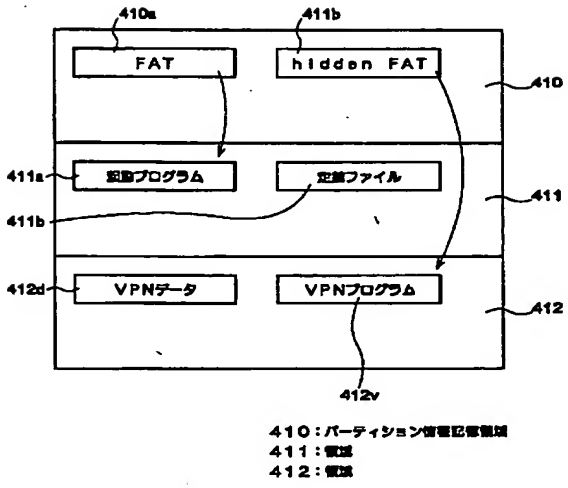
【図８】


<VPN構築処理>
<伝送機器>
<VPNクライアント>
スタート
スタート
1
パスワード入力画面表示
S1
入力?
NO
YES
S3
パスワード受信?
NO
YES
S21
伝送機器300へ送信
S5
判定部へ与える
S23
S7
パスワード一致信号受信?
NO
YES
S15
メッセージ表示
S25
判定部から一致信号?
NO
YES
S27
VPNデータ取得要求送信
S9
一致信号送信
不一致信号送信
S35
1
応答?
NO
YES
S11
VPNデータ取得要求有?
NO
YES
S31
メモリへ受信したVPNデータをセット
S13
VPNデータ送信
S33
2
エンド
HSS01808

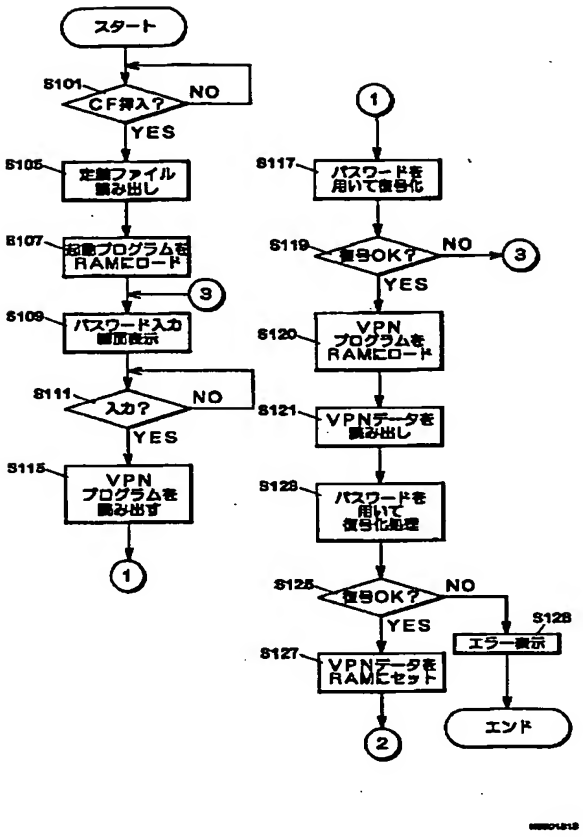
【図９】


<VPNクライアント>
<VPNサーバ>
スタート
3
S61
要求受信？
NO
4
YES
S63
リストに存在？
NO
YES
S64
直前VPNクライアントIPアドレス書込み
S65
復号化して転送
破棄（無視）
S67
2
S41
NO
送信要求？
YES
S43
VNPサーバへの要求？
NO
YES
S45
暗号化して送信
破棄（無視）
S47
S51
要求受信？
NO
2
YES
S53
一致？
NO
YES
S55
復号化してアプリケーションへ
破棄（無視）
S57
2
4
S71
送信要求？
NO
3
YES
S73
リストに存在？
NO
YES
S75
暗号化して送信
破棄（無視）
S77
3
HSS01809

【図１２】

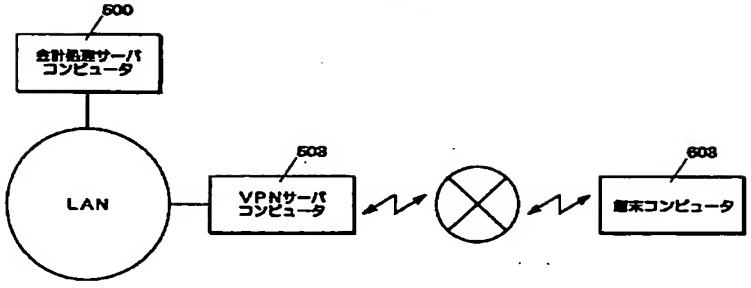


【図１３】



【図１４】

<従来技術>



フロントページの続き

(72)発明者　柴山　裕子
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内

(72)発明者　岡田　健一
大阪府大阪市中央区内本町２丁目４番16号　株式会社日立システムアンドサービス内

(72)発明者　小坂　達也
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(72)発明者　源田　浩一
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(72)発明者　植野　圭二
大阪府大阪市中央区内本町２丁目４番16号　株式会社日立システムアンドサービス内

Ｆターム(参考)　5B085 AA01 AE00 AE29 BE01 BG07
5J104 AA07 AA16 EA04 EA16 EA26
KA01 NA02 NA05 PA07